REMARKS

The February 13, 2006 Office Action was based upon pending claims 1 and 5-9. This amendment amends Claims 1, 5, 8, and 9. Thus, after entry of this amendment Claims 1 and 5-9 are pending and presented for further consideration.

In the February 13, 2006 Office Action, the Examiner rejected Claims 1, 5, and 8 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Publication No. 2001/0039659 to Simmons et al. ("the Simmons publication") in view of U.S. Patent Publication No. 2003/0046366 to Pardikar et al. ("the Pardikar publication") and further in view of the article "Applied Cryptography" to Schneier ("the Schneier article").

The Examiner further rejected Claims 6 and 9 under 35 U.S.C. 103(a) as being unpatentable over the Simmons publication in view of the Pardikar publication in view of the Schneier article and further in view of U.S. Patent No. 6,789,195 to Prihoda et al. ("the Prihoda patent").

The Examiner further rejected Claim 7 under 35 U.S.C. 103(a) as being unpatentable over the Simmons publication in view of the Pardikar publication in view of the Schneier article and further in view of U.S. Patent No 6,094,721 to Eldridge et al. ("the Eldridge patent").

Reconsideration of the pending claims as amended is respectfully requested.

REJECTION OF CLAIMS 1, 5, and 8 UNDER 35 U.S.C. § 103(a)

The Examiner rejected Claims 1, 5, and 8 under 35 U.S.C. 103(a) as being unpatentable over the Simmons publication in view of the Pardikar publication and further in view of the Schneier article.

Claim 1

Simmons does not teach the transaction server checking a file attribute of the requested data to determine whether the requested data is encrypted. Further, Simmons does not teach the transaction server encrypting the data with the public encryption key when the data is not encrypted. Further yet, Simmons does not teach the transaction server sending the encrypted data to the player/receiver.

Instead, in Simmons, the transaction receiver is between the player/receiver and the content provider site for information flowing from the player/receiver to the content

provider site and is not involved in the data transfer between the content provider site and the player/receiver. The transaction server receives the file request and the encryption key from the player/receiver and sends the file request and the encryption key to the content provider. The content provider encrypts the requested files without determining whether the requested files are already encrypted. Further, the content provider, and not the transaction server, sends the encrypted file to the player/receiver. See paragraph 41.

Pardikar does not teach the server encrypting the data with the public encryption key when the data is not encrypted. Instead, Pardikar teaches away from the server encrypting the data. In paragraph 74, Pardikar discloses problems with having the server encrypt the file data. To avoid the problems, Pardikar's server is not given the encryption key. See paragraph 75.

Schneier, like Simmons, does not teach the network server checking a file attribute of the requested data to determine whether the requested data is encrypted. Further, Schneier, like Simmons and Pardikar, does not teach the network server encrypting the data with the public encryption key when the data is not encrypted. Further yet, Schneier, like Simmons and Pardikar, does not teach the network server sending the encrypted data to the client computer system.

In contrast, in an embodiment, a method of transferring files over a computer network from a network server to a client computer system comprises receiving at a network server a request for data from a client computer system, checking a file attribute of the requested data using the network server to determine whether the requested data is encrypted, automatically retrieving using the network server a public encryption key from the client computer system when the data is not encrypted, encrypting the unencrypted data with the public encryption key automatically and without user intervention, and sending the encrypted data to the client computer system.

Because the references cited by the Examiner do not disclose, teach or suggest checking a file attribute of the requested data by the network server to determine whether the requested data is encrypted, automatically retrieving using the network server a public encryption key from the client computer system when the data is not

encrypted, encrypting the unencrypted data with the public encryption key, and sending the encrypted data to the client computer system, Applicant asserts that Claim 1 is not obvious in view of Simmons, Pardikar, and Schneier, alone or in combination. Applicant therefore respectfully submits that Claim 1 is patentably distinguished over the cited references and Applicant respectfully requests allowance of Claim 1.

Claims 5 and 8

Although Claims 5 and 8 have different language than Claim 1, Claims 5 and 8 are believed to be patentable for similar reasons (where applicable), and because of the different features recited therein.

REJECTION OF CLAIMS 6, 7, and 9 UNDER 35 U.S.C. § 103(a)

The Examiner further rejected Claims 6 and 9 under 35 U.S.C. 103(a) as being unpatentable over the Simmons publication in view of the Pardikar publication in view of the Schneier article and further in view of the Prihoda patent.

The Examiner further rejected Claim 7 under 35 U.S.C. 103(a) as being unpatentable over the Simmons publication in view of the Pardikar publication in view of the Schneier article and further in view of the Eldridge patent.

Claims 6, 7, and 9

Claims 6 and 7, which depend from Claim 5, and Claim 9, which depends from Claim 8, are believed to be patentable for the same reasons articulated above with respect to Claims 5 and 8, respectively, and because of the additional features recited therein.

SUPPLEMENTAL INFORMATION DISCLOSURE STATEMENT

Submitted concurrently herewith is a Supplemental Information Disclosure Statement and form PTO/SB/08 Equivalent citing 51 references which were cited in related U.S. Patent Application Nos. 09/277,482, 10/962,997, and 09/277,335. Applicant respectfully requests the Examiner to consider the pending claims in connection with these references in order to make them of record.

CONCLUSION

Although amendments and cancellations have been made, no acquiescence or estoppel is or should be implied thereby. Rather, the amendments and cancellations are made only to expedite prosecution of the present application, and without prejudice to presentation or assertion, in the future, of claims on the subject matter affected thereby. Furthermore, any arguments in support of patentability and based on a portion of a claim should not be taken as founding patentability solely on the portion in question; rather, it is the combination of features or acts recited in a claim which distinguishes it over the prior art.

In view of the foregoing, the present application is believed to be in condition for allowance, and such allowance is respectfully requested. If further issues remain to be resolved, the Examiner is cordially invited to contact the undersigned such that any remaining issues may be promptly resolved. Also, please charge any additional fees, including any fees for additional extension of time, or credit overpayment to Deposit Account No. 11-1410.

Respectfully submitted,

KNOBBE, MARTENS, OLSON & BEAR, LLP

Dated: May 12, 2006

By: Karen J. Lenker

Karen J. Lenker
Registration No. 54,618
Agent of Record
Customer No. 20,995
(949) 760-0404

2569773
050206